CONFIDENTIAL

How to Protect Your Computer from Hackers, Viruses and Spies

Online Safety Is Important

We must secure our computers with technology in the same way that we secure the doors to our homes

http://www.staysafe.org

Leading Threats to PC Security

Viruses/Worms

Software programs designed to invade your computer, and copy, damage or delete your data

Trojan Horses

Viruses that pretend to be programs that help you while destroying your data and damaging your computer

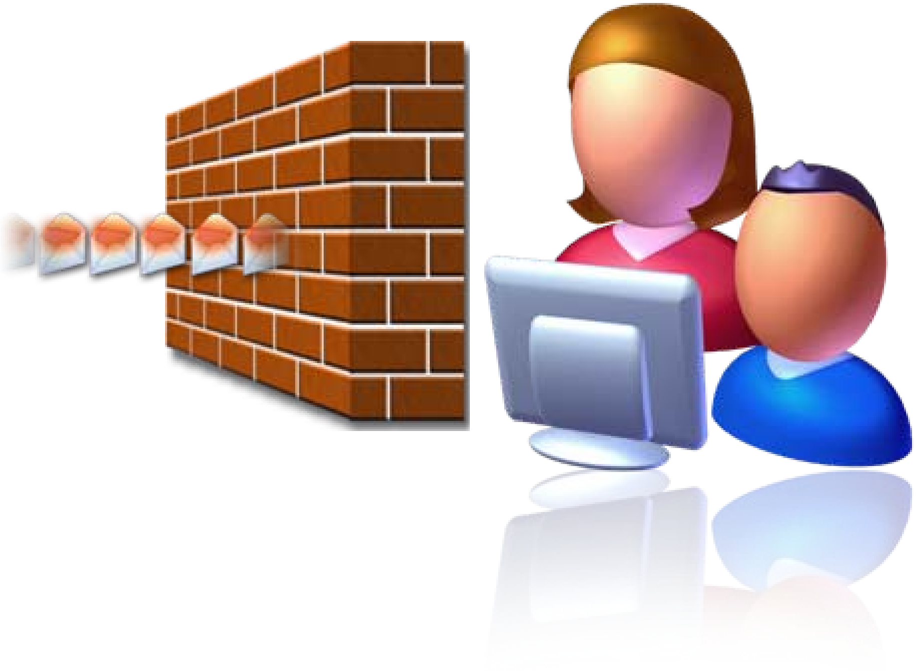
Spyware

Software that secretly watches and records your online activities or send you endless pop-up ads

Four Steps To Protect *Your Computer*

1. Turn on an Internet firewall
2. Keep your operating system up to date
3. Install and maintain antivirus software
4. Install and maintain antispyware software

Turn on an Internet Firewall



An Internet firewall is like a moat around a castle, creating a barrier between your computer and the Internet

Keep Your Operating System Updated

- Install all security updates as soon as they are available
- Automatic updates provide the best protection

Install Antivirus Software

Don’t let it expire

- Anti-virus software can detect and destroy computer viruses before they can cause damage
- Just like flu shots, for anti-virus software to be effective, you must keep it up to date

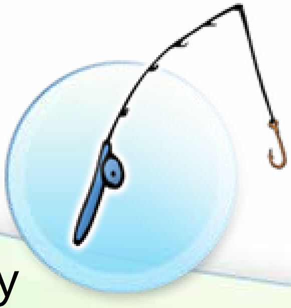
Install And Maintain Antispyware Software

Use anti-spyware software so unknown people cannot lurk on your computer and potentially steal your information

Four Steps To Protect *Your Computer*

1. Turn on an Internet firewall
2. Keep your operating system up to date
3. Install and maintain antivirus software
4. Install and maintain antispyware software

Leading Threats to Personal Online Safety



Phishing

E-mail sent by online criminals that tries to trick you into revealing personal information

Spam

Unwanted e-mail, instant messages, e-cards, and other online communication

Hoaxes

E-mail sent by online criminals that tries to trick you into giving them money

Identity Theft

A crime where con artists get your personal information and access your cash and/or credit

Take Steps to Help Protect *Yourself*

1. **Practice** Internet behavior that lowers your risk

2. **Manage** your personal information carefully

3. **Use** technology to reduce nuisances, and raise the alarm when appropriate

Delete Spam without Opening It

- Never reply to spam
- Technology can help you identify spam so you can delete it
- Many Internet providers delete it for you

Be on the Lookout for Scams!

There are signs that you can alert you of e-mail scams

- Alarmist messages and threats of account closures
- Promises of big bucks for little effort
- Deals that sound too good to be true
- Misspellings and grammatical errors

Don’t Share Personal Information

- Delete e-mails that request personal information
- Do not use e-mail or instant messages to share personal information

Use Strong Passwords

- Keep passwords private and create ones that are hard to “crack”
- Never share your passwords with friends or be tricked into giving them away

More Safe Internet Behavior

Back up your files regularly

Think before you click

Read website privacy statements

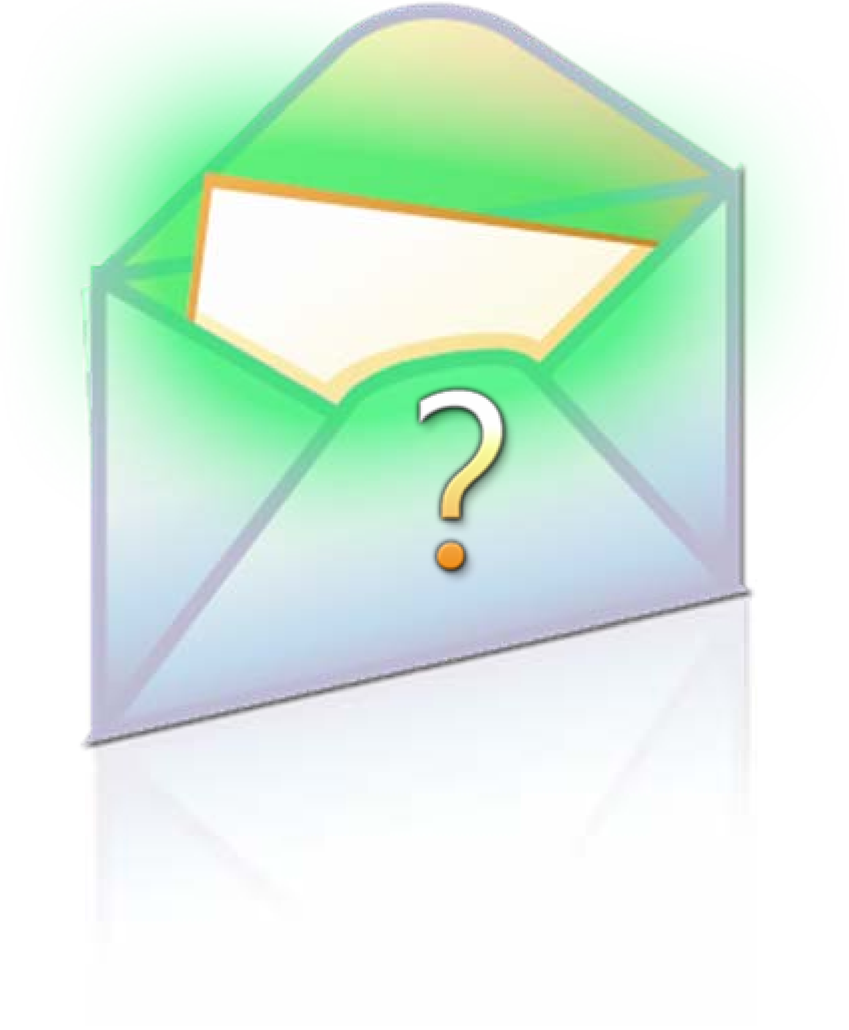
Close pop-ups using red “X”

Back Up Your Files

- Save to CD, DVD or flash drive
- Use a Web-based backup service

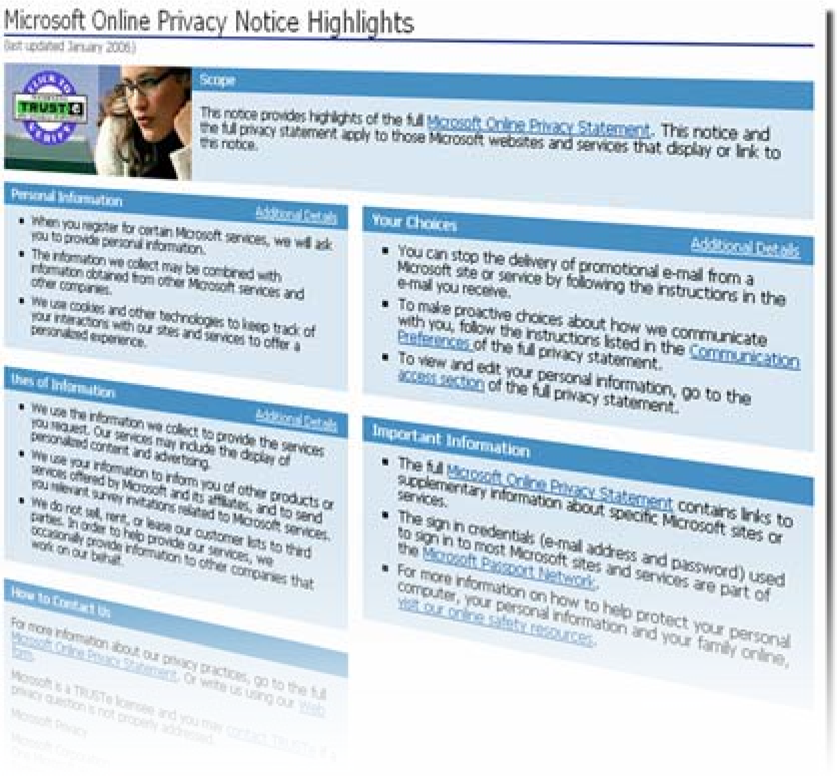
Think Before You Click

- Don’t open e-mail attachments unless you know what they contain and who sent them
- Only download files from websites you trust



Read Privacy Statements

Understand what you are getting before you agree to download or share your personal information



Microsoft Online Privacy Notice Highlights

(last updated January 2006)

Scope

This notice provides highlights of the full Microsoft Online Privacy Statement. This notice and the full privacy statement apply to those Microsoft websites and services that display or link to this notice.

Personal Information

Additional Details

- When you register for certain Microsoft services, we will ask you to provide personal information.
- The information we collect may be combined with information obtained from other Microsoft services and other companies.
- We use cookies and other technologies to keep track of your interactions with our sites and services to offer a personalized experience.

Uses of Information

Additional Details

- We use the information we collect to provide the services you request. Our services may include the display of personalized content and advertising.
- We use your information to inform you of other products or services offered by Microsoft and its affiliates, and to send you relevant survey invitations related to Microsoft services.
- We do not sell, rent, or lease our customer lists to third parties. In order to help provide our services, we occasionally provide information to other companies that work on our behalf.

How to Contact Us

For more information about our privacy practices, go to the full Microsoft Online Privacy Statement. Or write us using our Web form.

Microsoft is a TRUSTe licensee and you may contact TRUSTe if a privacy question is not properly addressed.

Microsoft Privacy

Microsoft Corporation

Your Choices

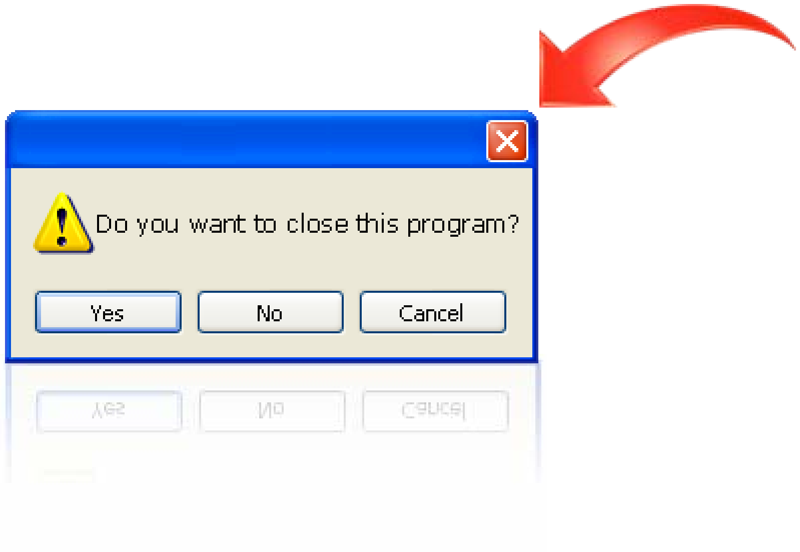
Additional Details

- You can stop the delivery of promotional e-mail from a Microsoft site or service by following the instructions in the e-mail you receive.
- To make proactive choices about how we communicate with you, follow the instructions listed in the Communication Preferences of the full privacy statement.
- To view and edit your personal information, go to the access section of the full privacy statement.

Important Information

- The full Microsoft Online Privacy Statement contains links to supplementary information about specific Microsoft sites or services.
- The sign in credentials (e-mail address and password) used to sign in to most Microsoft sites and services are part of the Microsoft Passport Network.
- For more information on how to help protect your personal computer, your personal information and your family online, visit our online safety resources.

Close Pop-ups Using Red “X”


Do you want to close this program?

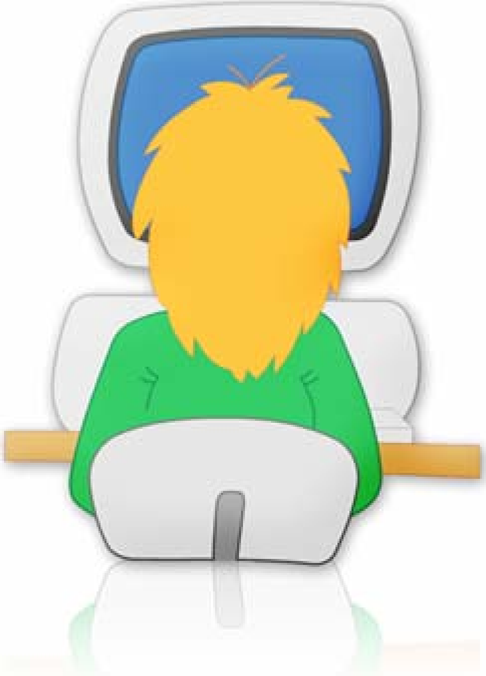
- Always use the red “X” in the corner of a pop-up screen
- Never click “yes,” “accept” or even “cancel”, because it could be a trick that installs software on your PC

Take Steps to Help Protect *Your Family*

1. **Talk** with your kids about what they do online
2. **Keep** personal information private
3. **Set** clear rules for Internet use
4. **Use** family safety software

Pay Attention to What Your Kids Do Online

- Keep the computer in a central area
- Get to know how your kids use the Internet
- Let your kids be the teacher
- Teach kids to trust their instincts
- And to report any problems



Keep Personal Information Private

- Teach children never to share personal information online without permission
- Monitor your children’s online activities
- Teach your children to report suspicious activity
- Help children choose appropriate screen names and e-mail addresses

http://www.staysafe.org

For More Information

www.geeksquad.com/centralintelligence

www.microsoft.com/protect

www.staysafe.org

www.getnetwise.org

staysafe.org
Microsoft
security at home
Traveling with your laptop
7 security tips to remember on the road.
protect your computer
protect yourself
you are running Windows XP SP2
How to use the Windows Security Center
How-to articles
Get support

Go Ahead. Use Us.

Your potential. Our passion.™

The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation.
MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.